Claims

What is claimed is:

1. A mobile device for providing certificate based cryptography, the mobile device comprising:

a receiver operative to receive a wireless transmission of a certificate revocation notification over a broadcast channel;

an authenticator operative to receive the certificate revocation notification, the authenticator operative to authenticate signed comparison data included within the certificate revocation notification; and

an updater, coupled to the authenticator, the updater operative to update data representing at least one private or public key based on the certificate revocation notification.

2. The mobile device of claim 1 wherein the certificate revocation notification includes a certification authority identifier, revocation reason data, and data representing a certificate of interest.

3. The mobile device of claim 2 further comprising a searcher operative to receive the certification authority identifier from the authentication module, the searcher operative to retrieve a stored certificate corresponding to the certification authority identifier.

4. The mobile device of claim 3 wherein the authenticator further includes a first verification value generator operative to generate a first verification value based on the signed comparison data and the data representing a certificate of interest; a second verification value generator operative to generate a second verification value based on the certification authority identifier and the revocation

reason data; and a comparator operative to compare to the first verification value and the second verification value.

5. The mobile device of claim 2 wherein the signed comparison data is a compressed representation of the combination of the certification authority identifier and the revocation reason data using a hash algorithm.

6. The mobile device of claim 2 wherein the data representing a certificate of interest is at least one of: a certificate and a universal resource locator.

7. The mobile device of claim 1 wherein the channel is at least one of: a dedicated broadcast channel and a channel assigned a predetermined port identifier in a messaging system.

8. The mobile device of claim 7 wherein the messaging system is at least one of a: short messaging system and an extended messaging system.

9. The mobile device of claim 1 further comprising:

a user interface coupled to the searcher, the user interface operative to receive user display information regarding the certificate revocation notification and the user interface coupled to the updater wherein the updater is operative to update the data representing at least one private or public key based on a user input received by the user interface module.

10. A method for providing certificate based cryptography in a mobile device, the method comprising:

receiving a certificate revocation notification from a wireless transmission over a broadcast channel;

authenticating the certificate revocation notification; and

updating data representing at least one private or public key based on the certificate revocation notification.

11. The method of claim 10 wherein the certificate revocation notification includes a certification authority identifier, revocation reason data, signed comparison data and data representing a certificate of interest.

12. The method of claim 11 further comprising generating a first verification value from the signed comparison data and the data representing a certificate of interest; generating a second verification value based on the certification authority identifier and the revocation reason data; and comparing the first verification value with the second verification value.

13. The method of claim 12 further comprising: accessing data representing at least one private or public key; and retrieving a certificate based on the certification authority identifier.

14. The method of claim 13 further comprising displaying friendly name data extracted from the certificate revocation notification and the revocation reason data; and querying an end user to remove the certificate from the data representing a certificate of interest.

15. The method of claim 11 wherein the data representing a certificate of interest is at least one of: a certificate and a universal resource locator.

16. The method of claim 10 wherein the broadcast channel over which the wireless transmission of the certificate revocation notification is received is at least one of: a dedicated broadcast channel and a messaging system channel.

17. The method of claim 18 wherein a messaging system using the messaging system channel is at least one of a: short messaging system and an extended messaging system.

18. A method for providing certificate based cryptography in a plurality of mobile devices, the system comprising:

generating a certificate revocation notification from a certification authority, wherein the certification authority is within a domain of trust; and

wirelessly transmitting the certificate revocation notification to the plurality of mobile device using a broadcast channel.

19. The method of claim 18 wherein the certificate revocation notification includes a certification authority identifier, revocation reason data, signed comparison data and data representing a certificate of interest.

20. The method of claim 18 wherein the broadcast channel is a messaging system broadcast channel and the messaging system is at least one of: a short messaging system and an extended messaging system.

21. The method of claim 18 wherein when the broadcast channel is a dedicated certificate revocation notification broadcast channel.

22. A method for providing certificate based cryptography in a mobile device, the method comprising:

receiving a certificate revocation notification from a wireless transmission over a broadcast channel, wherein the certificate revocation notification includes a certification authority identifier, revocation reason data, signed comparison data and data representing a certificate of interest;

authenticating the certificate revocation notification, wherein the authenticating includes:

generating a first verification value from the signed comparison data and the data representing a certificate of interest;

generating a second verification value based on the certification authority identifier and the revocation reason data; and

comparing the first verification value with the second verification value; and

updating data representing at least one private or public key based on the certificate revocation notification;

23. The method of claim 22 further comprising: accessing data representing at least one private or public key; retrieving a certificate based on the certification authority identifier; displaying friendly name data extracted from the certificate revocation notification and the revocation reason data; and querying an end user to remove the certificate from the data representing a certificate of interest.

24. The method of claim 22 wherein the broadcast channel over which the wireless transmission of the certificate revocation notification is received is at least

one of: a dedicated broadcast channel and a channel assigned a predetermined port identifier in a messaging system.